MANAGEMENT HANDBOOK ON **TRAINING PROCEDURES IN PUBLIC TRANSPORT**

SAFEBUS

This project was funded by the European Union's Internal Security Fund – Police, under the Grant Agreement No. 101034233

TABLE OF CONTENTS

(1)

INTRODUCTION

Transport operators are responsible for the safety and wellbeing of their passengers. Besides providing safe and reliable transport, this also includes protecting them from crime and potential acts of terrorism.

This handbook is intended for security managers and provides guidance for measures and policies to:

- **Assess** the potential exposure of a public transport organisation to terrorist activity along with the state of protection.
- **Prevent** terrorist attacks and limit the damage that could be caused.
- **Detect** suspicious situations and malicious intent.
- **Respond** to emergencies.

The set-up and context of public transport operators vary widely, security plans and policies need to take the individual situation into account.

This handbook intends to be a blueprint, outlining aspects that need to be addressed and best practices that may help to compile company-specific security plans and procedures.

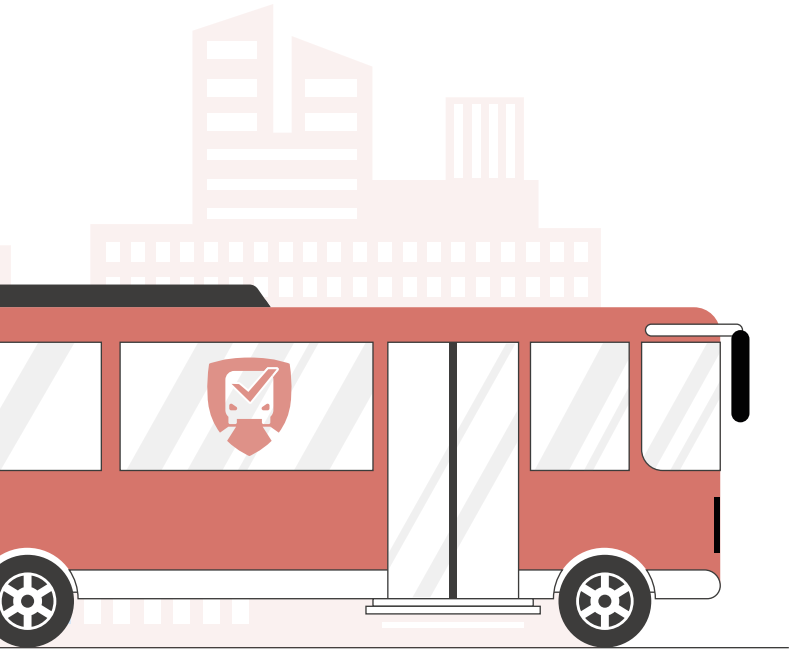
(2)

ANTI-TERRORISM GUIDE

CONTEXT

Terrorism means the use of violence or other criminal acts as justified means to achieve political goals. Unfortunately, public transport systems have repeatedly been the target of terrorist activities, aiming to disrupt operations and sabotage mobility services.

Potential targets for terrorist activities could be our vehicles and infrastructure. The objective could also be to cause harm to people using public transport.
As transport operators, we are responsible for the safety and wellbeing of our passengers and staff. This includes reasonable measures to prevent incidents, but also being prepared to respond to incidents and limit the damage as much as possible.



THREATS AND TARGETS

RELEVANT ASSETS

Bus operation requires a variety of assets to be able to provide mobility services to their customers, some publicly accessible, some protected and with restricted access only. Relevant assets include:

- **Passenger-related assets,** including stations and interchanges, stops, sales and information centres, possibly luggage storage facilities. These facilities are open to the public with limited possibilities for access control.
- **Operation-related assets,** which include vehicles, depots, and workshops, as well as fuel supply facilities. The accessibility to these facilities varies.
- **Support assets** comprise control rooms, staff and service facilities and administrative buildings. They are comparable to assets of any other business and are not open to the public.
- **Digital assets** are increasingly critical for bus operations. They may include operational control systems, passenger information and control systems as well as business management systems for ticketing, payment and booking. Physical access to these assets is normally integrated in operation-related or support assets, which are not open to the public.

INCIDENT SCENARIOS

Based on recent general events and incidents specifically the public transport sector, the following (non-exhaustive) list of scenarios may be considered.

- **Improvised explosive device (IED)** – a makeshift explosive device that be concealed in ordinary luggage or hidden out of sight, possibly under seats or in trash receptacles. IEDs may be triggered with a timer or remotely, there is no need for the attacker to be in the vicinity.
- **Suicide attack** – an attacker carries the explosive device directly to the bus system and sets it off directly.
- **Firearms** – an attacker shooting targeted or at random, from a distance or close-by.
- **Stabbing** – attack using knifes and blades to attack people at close distance.
- **Sabotage** – vandalism, theft or manipulation of equipment aiming to compromise operational capacity and safety.
- **Arson** – deliberate setting fire to destroy assets.
- **Car-borne attack** – using an external vehicle to crash into passengers or installations of the bus operator.
- **Bus-borne attack** – using a bus to crash into people anywhere.
- **Hostage-taking / Hijacking** – an attack holding people with direct threat to their lives, in stations or on board of vehicles.
- **Bomb threat** – threat to detonate an explosives device in the bus system, whether or not such device actually exists.
- **Cyber-attack** – attack targeting computer information systems, networks, or devices.
- **CBRN attack** – attack using chemical, biological radiological or nuclear substances.

SECURITY POLICIES AND SAFEGUARDS

SECURITY CONCEPT ELEMENTS

A number of tools and safeguards are available to protect public transport. A sound security concept makes use of all of them to develop an efficient mix.

Infrastructure measures lay the foundation to deter any attack and limit the potential damage caused. They comprise:

- The construction and material used to build any asset;
- The layout, design and spatial organisation of any area, as well as;
- The distribution of guard posts and access control gates.

Technology tools help securing widespread areas, centralising monitoring and efficient dispatching of staff. They include:

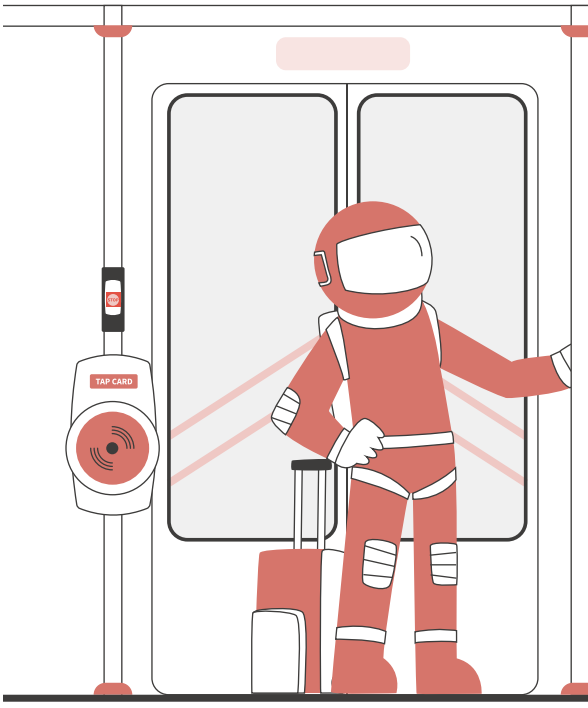
- CCTV surveillance, video analytics and forensics;
- Emergency poles and help buttons;
- Security technology, such as locks and keys or sensors to detect potentially suspicious situations;
- Communication technology to coordinate incident verification and response.

Staff is a key factor in security concepts, thus includes dedicated security staff, but also operational and customer service staff. Relevant aspects are:

- Roles and responsibilities;
- Schedules and procedures;
- Training and education.

Organisational measures provide the framework for the entire security concept and include:

- Monitoring;
- The security, emergency management and crisis organisation;
- The assignment of roles and responsibilities, also guiding the cooperation between security and operations;
- Security partnerships with authorities, emergency responders and business partners.



SECURITY MANAGEMENT PRINCIPLES

PREVENTION in public transport security is critical. Prevention measures aim to identify and mitigate potential threats before they can cause any harm and to deter potential offenders from attempting to attack and disrupt public transport systems.

Basically, two strategies are available to protect these assets- **access control** to create a deterrent and monitor who is entering a facility, and **hardening infrastructure** to limit the damage that could be cause by a potential attack.

DETECTION measures are an important complement to prevention measures. They aim to **identify potential security threats** and to **facilitate a quick and targeted response.**

Staff plays a key role in the detection of potential threats but given the extension of operated assets and network in public transport, technology provides important support to monitor the entire territory.

PREPAREDNESS acknowledges that prevention may fail and comprises emergency plans outlining roles and responsibilities, communication protocols and response procedures as well as business continuity planning.

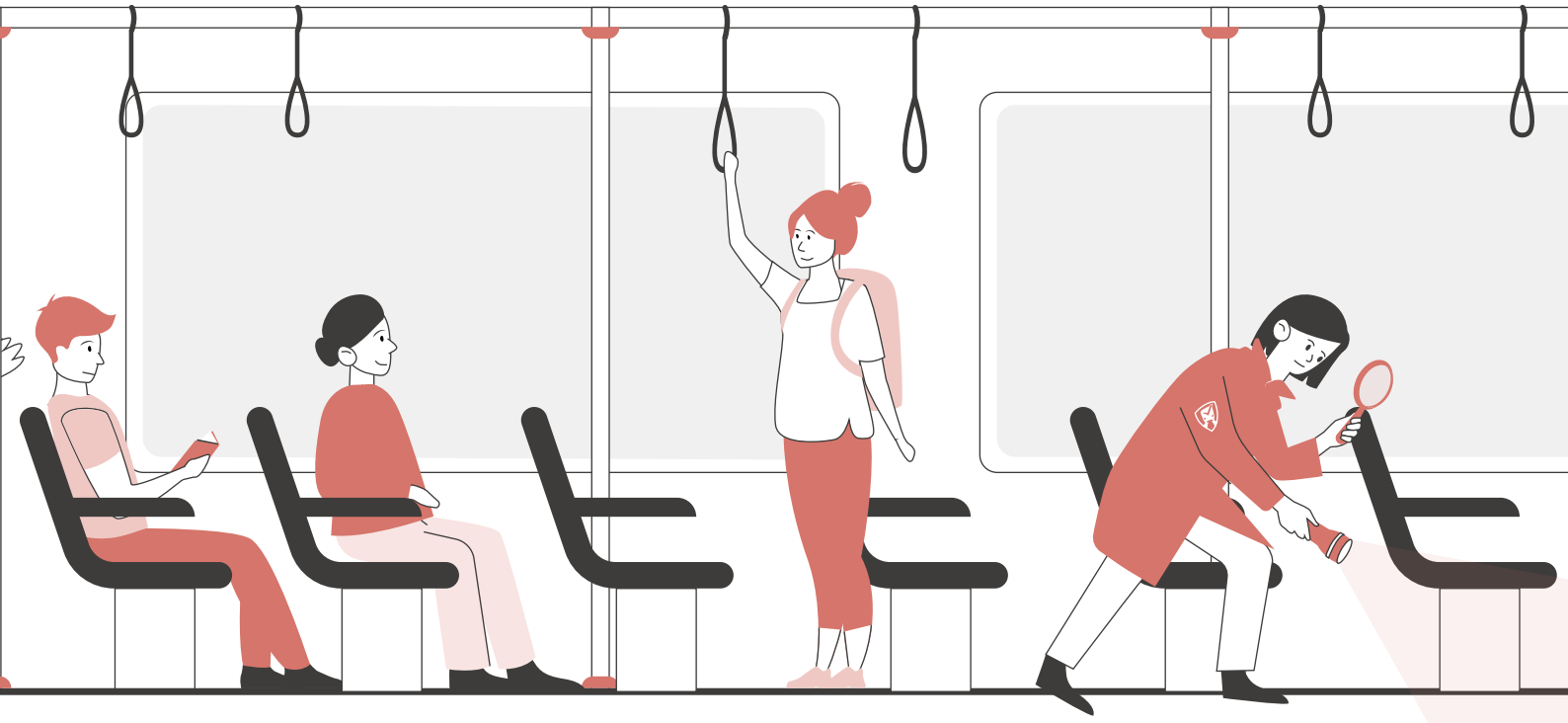
Staff needs regular **training and exercises** to be familiar with their roles and responsibilities to ensure an efficient response to emergencies. **Business continuity planning** need to ensure limiting the operational impact of any incident and anticipate contingency plans.

INCIDENT RESPONSE involves the mobilisation of resources and personnel to respond to an emergency. Terrorist attacks are likely to escalate an emergency to a crisis situation.

Beyond activating internal emergency communication protocols and deploying internal response teams, crisis management requires the activation of a crisis cell and coordination with external emergency responders.

After any emergency, it is important to conduct an evaluation to review how the emergency response could be improved and assess the potential for improved prevention.

As transport operators, we are responsible for the safety and wellbeing of our passengers and staff.



3

RISK ASSESSMENT AND MONITORING

THREAT ASSESSMENT

The baseline for any security concept and plan is a thorough assessment of threats and risks, which the own organisation is potentially exposed to. Although public transport is considered a target for terrorist activities, threat levels vary depending on several factors, such as the general political situation in your country/region, the size and economic importance of your city or recent attacks carried out elsewhere.

The threat picture needs to be regularly validated as the target priorities and modus operandi of potential offenders continuously change. Also, planned high-level events such as major sports events or political gatherings may elevate the threat level temporarily.
Threat levels should be assessed in cooperation with the responsible authorities, who will have a deeper insight into the current global and local situation.

RISK ASSESSMENT

Risk and vulnerability assessments help bus operators identify potential weaknesses and prioritise investment in upgrading their facilities. These assessments should be regularly repeated to reflect structural changes or construction activities, as well to be aligned with the emergence of new threats and development of modus operandi. It is important not to limit risk and vulnerability assessment to critical assets, but also to consider public spaces needed for the operation of bus services.

- The COUNTERACT project, coordinated by UITP, has elaborated a **methodology for risk and vulnerability assessment** specifically tailored to the public transport sector. This methodology has been continuously updated to the evolving threat situation and is recommended by UITP for use by public transport operators.

RISK MONITORING

The security risk environment, also for bus operations, is continuously changing. New threat scenarios may arise, the renovation of company assets may create new potential vulnerabilities, events or new construction projects in the operating area may result in new potential targets. It is therefore important to continuously monitor risk to help ensure that risk management strategies are effective and aligned with the changing risk environment.

- At the **corporate level**, close cooperation with the relevant authorities can help to learn as early as possible about changes in the threat assessment and potential consequences for the operation of bus services.
- At the **operational level**, risk and vulnerability assessments need to be regularly repeated, to reflect infrastructure changes, the acquisition of new vehicles, technology development, and to carry out stress tests in line with the evolution of incident scenarios as communicated by the authorities or as witnessed in public transport operations elsewhere.
- At the **site level**, regular security audits help establish whether existing security safeguards are still functional and appropriate to protect company assets.

Risk and vulnerability assessments help bus operators identify potential weaknesses and prioritise investment in upgrading their facilities.

(4)

BUILDING SECURITY

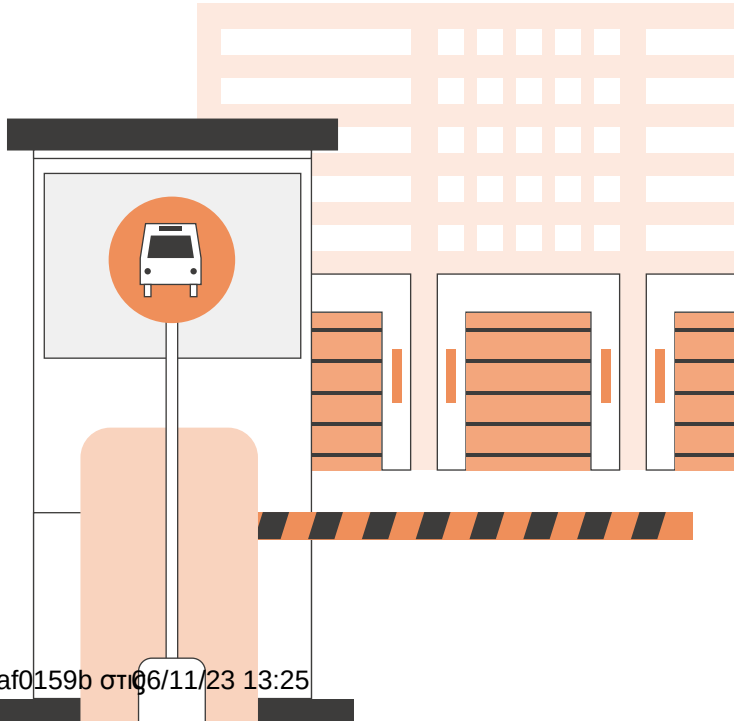
PUBLIC FACILITIES

Passenger-related facilities are publicly accessible and need to be able to process large numbers of people efficiently. The potential for access control measures is limited. Key protection principles for bus stations and stops include monitoring to identify potentially suspicious situations and hardening the infrastructure to deter and limit the consequences of a potential attack.

DESIGN AND INFRASTRUCTURE

Standards and guidelines for station layout and material have evolved a lot during recent years and are followed for new structures or the upgrading of existing facilities and equipment. In general, however, public transport systems are not new and involve legacy infrastructure directly embedded into the public space. Key measures to be considered in bus stations include:

- **Clear lines of sight** in any passenger related facility help monitoring the area, avoid creating areas of concealment and facilitate a speedy evacuation if needed. Furniture, vending machines and information screens and boards should be made of vandalism-proof material and be positioned to not block any view.
- **Adequate lighting** is needed for good orientation and overview for passengers. It also supports surveillance and the monitoring of bus stations by CCTV cameras.
- **The station layout** should separate left luggage and other storage facilities from concourses, platforms, and passenger flow routes to minimise the impact of a potential explosion.
- **Locks and seals** can prevent access to cup boards, equipment boxes or access to technical installations, which could potentially be used as places of concealment. Where locks cannot be installed, tamper-evident seals should be fitted.
- Litter bins must be considered a place of easy concealment for dangerous objects and substances. **Clear plastic sacks** suspended from metal hoop sack holders that allow for maximum transparency are considered best practice. If possible, litter bins should be placed into areas covered by CCTV to monitor them. Litter bins should be regularly emptied to make best use of the sacks' transparency.
- Waiting areas and bus stops should be protected against vehicle borne attacks without jeopardising an obstacle-free access for passengers. Protection could be achieved by **physical barriers**, such as bollards or planters as well as elevated curbs.
- Transparent structures, such as bus shelters, should have **glazing protection** to avoid flying or falling glass in case of an explosion. Laminated glass or anti-shatter film to retrofit existing structures can also help to prevent vandalism and graffiti.



Key protection principles for bus stations and stops include monitoring to identify potentially suspicious situations.

TECHNOLOGY

Technology tools can substantially help improving the protection of bus systems, with closed circuit television (CCTV) being the most used and important one in public transport.

- **CCTV cameras** can essentially support the monitoring of stations, which are often too widespread to be efficiently covered by personnel. Cameras should continuously give an overview of the situation within a station. Sensitive locations, such as emergency help points, equipment boxes or access points to technical installations should be a special focus. In order to avoid tampering or the loss of evidence in case as a result of cameras destroyed during incidents, they should be positioned to cover each other.
- **Real-time monitoring** of camera images in the control room allows using CCTV for alarm verification and incident management, supporting the efficient use of personnel.
- **CCTV recordings and audio footage** are essential evidence in the investigation of any situation. Recordings are stored for a legally binding period, before being overwritten. They need to be of sufficient quality to be admissible in legal procedures.
- **Video analytics** in CCTV cameras can help identifying suspicious situations. The open nature of stations and often high density of people make for challenging conditions, but the technology is developing. Most common algorithms tested for public facilities include detecting abandoned items, aggressive behaviour, or unusual passenger movements.

Sensors and alarms can help detecting potentially suspicious situations. Most common installations concern intrusion alarms protecting doors and locks. Sensors can detect smoke or chemical substances.

Technology can also support passengers and staff in need for help.

- **SOS intercoms** installed at major stations and interchanges enable passengers and staff to call for help. Often, these intercoms are equipped with cameras to prevent misuse.
- **Body cameras** can be used to protect staff. They act as a deterrent against aggressions, their live images help control room staff to understand situations and recordings provide evidence in the investigation of incidents.

STAFF AND PROCEDURES

Personnel plays multiple security-relevant roles in stations. Their presence acts as a deterrent against potential offenders and reassurance for passengers, helping to create a managed space. Attentive staff members can efficiently meet passenger service and security objectives.

The pro-active security role of staff in stations includes:

- **Vigilance** of the public space to identify potentially suspicious situations. This includes unusual and inappropriate behaviour as well as unattended items. Staff needs to be familiar with the concepts of suspicious behaviour and items. Any concern should be reported to enable clarification or a follow-up by security staff or the police. To avoid false alarms, training should be provided on how to recognise one's bias when assessing potential threats.
- **Regular security checks** patrolling of the station helps increasing the visibility of personnel. Patrols can be shared by staff members and could combine vigilance with customer engagement and regular checking of integrity of physical security measures. Security patrols should have a clearly outlined area to be covered with defined touch points and instructions (e.g., physically checking that a door is locked). Security patrols need to be unpredictable and should be recorded.

RESTRICTED FACILITIES

Access control to restricted facilities and equipment is key to ensure that only authorised personnel and material can enter a site via controlled entrance ways. Inside the premises, general vigilance helps to ensure reporting unusual presence, behaviour, and items.

DESIGN AND INFRASTRUCTURE

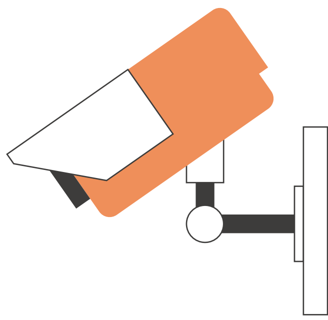
- Physical access barriers such as walls and fences should **protect the perimeter** of depots, workshops, or other restricted facilities. These barriers should be kept in good state of repair and could be complemented with intrusion sensors for extra protection.
- All doors between public and restricted areas should be locked or controlled. Restricted assets, such as depots should be equipped with **controlled access gates**, only allowing authorised people to enter.

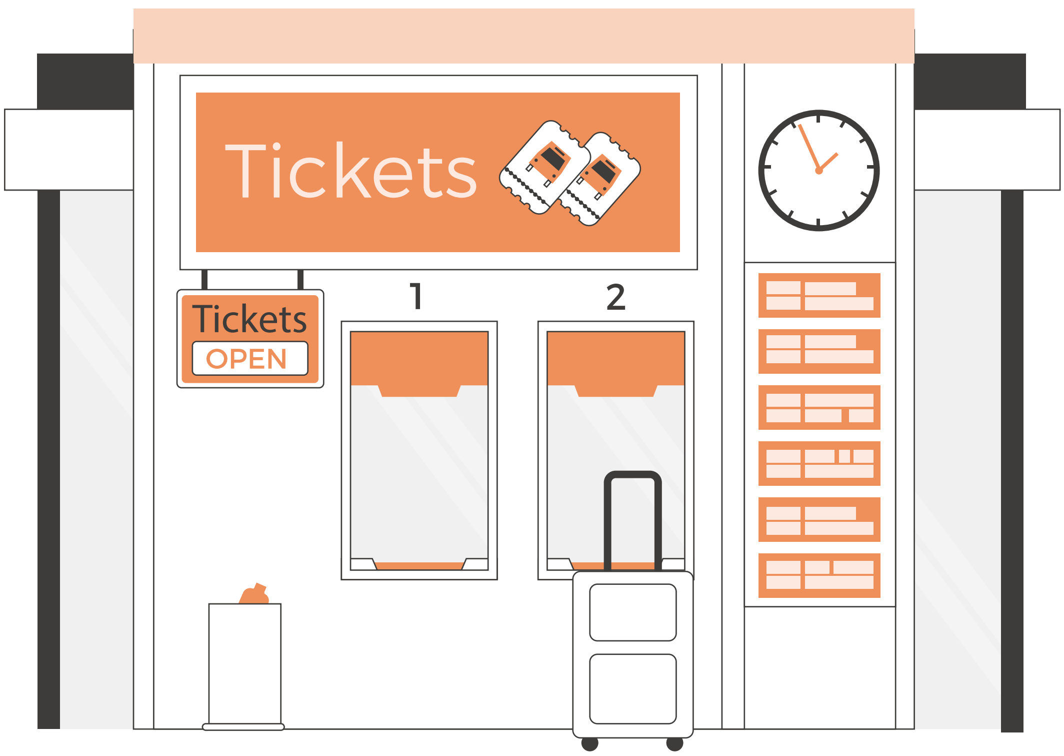
TECHNOLOGY

- **CCTV cameras equipped with night vision** can support intrusion detection by monitoring the inner and outer perimeter to prevent unauthorised access.
- **Geofencing** can create a virtual perimeter as extra protection or where physical barriers cannot be erected. This can help monitoring the surrounding of the facility or establishing a high security zone within a facility, such as the parking area of new rolling stock.
- **Video analytics** provides extra protection at times when restricted facilities are closed, and no operational activities take place.

STAFF AND PROCEDURES

- A **check-in procedure** should ensure that non-authorised staff and visitors are checked and registered. If private cars can be parked on the ground, they should be inspected including the luggage and be subject to a parking permit system.
- **Badges and permits** issued should be visibly displayed to identify any person or car as accredited. They should be worn visibly while people are inside restricted facilities. Clear sign in/out procedures also facilitate an evacuation if needed.
- **Buses and coaches should be checked** upon entering and leaving restricted facilities for service to ensure that no unattended item or unauthorised person is on board. These checks can be carried out by drivers and should be recorded.
- **Staff vigilance** and facility patrols, as in public facilities, are key to ensure identifying potentially suspicious situations. Unfamiliar people should be engaged to confirm their purpose and check-in. Staff needs to be familiar with the concepts of suspicious behaviour and items. Any concern should be reported to enable clarification or a follow-up by security staff or the police.





5

VEHICLE SECURITY

The protection of vehicles needs to consider preventing sabotage and theft as well as entering with dangerous items and substances.

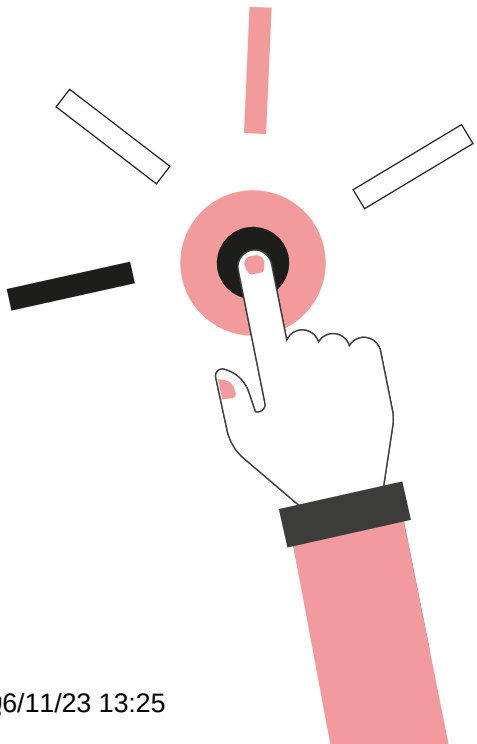
TECHNOLOGY

- **Smart bus ignition locks** can provide a further layer of protection with individual keys to ensure that only the planned and assigned driver can access and start the bus.
- Buses are often equipped with **alarm buttons for drivers**, enabling them to directly connect with the control room or dispatcher. Often these alarms are silent and allow the control room or dispatcher to listen into the situation to improve situational awareness.
- **Automated vehicle monitoring (AVM) systems** are increasingly common practice to manage and coordinate bus fleets. The continuous awareness of bus positions can help detecting deviations and suspicious movements.
- **Geofencing** can be used to monitor the position and movement of buses. It could be used to prevent the unauthorised removal of buses from unfenced depots or parking spots and alert in case of deviation of buses from their assigned route and service pattern.

STAFF AND PROCEDURES

- Access to buses and bus keys can be controlled by a **hand-over procedure,** handing out the keys to planned and assigned drivers only.
- Some form of access control can be carried by guiding passenger streams. Many operators had implemented the principle of **front-door-boarding-only** for buses; obliging passengers to pass the driver and buy or display a ticket. During the recent pandemic, however, this measure was revoked in many places for health and safety reasons.
- A **boarding procedure** for coach services can help ensure that only passengers with a valid and personalised ticket can enter a coach.
- A **passenger-baggage reconciliation** should take place before loading any item into the luggage compartment of coaches.

The protection of vehicles needs to consider preventing sabotage and theft as well as entering with dangerous items and substances.



(6)

ORGANISATIONAL SECURITY

SECURITY CULTURE

Building a strong security culture within an organisation requires leadership commitment, awareness of employees and continuous training. Security cannot be provided by the security department alone, it is a corporate responsibility, and every staff member plays a role.

Any security policy and concept can only be effective, if the expectations to all staff members are clear, relevant skills are explained and senior management is leading by example.

A positive security culture is creating an open, trusted atmosphere and encourages staff members to be proactive about reducing risks for everyone's benefit.

AWARENESS

It is key to acknowledge that security is not only the task of security managers and staff, but that every employee in every position has a role to play.

- **Awareness programmes** help remind staff of general rules, recognise suspicious situations and the procedures that must be followed.
- **Targeted campaigns** can contribute to maintaining general security awareness as well as refreshing the familiarity of rules and procedures.
- **Handouts and handbooks** distributed to staff or **posters** visible at the workplace can be important references to keep important contacts or procedures ready at hand.

PERSONNEL SECURITY

Personnel security addresses the risk of employees exploiting their legitimate access to company assets for unauthorised purposes. Like every organisation, also bus operators may be threatened by an insider.

This could be countered by a careful selection of staff to be employed, by defining clear procedures for work and instilling the discipline to follow those procedures and encouraging staff to be vigilant for suspicious behaviour.

- A **criticality analysis of staff positions** helps determine necessary access (e.g., control room) and use rights (e.g., vehicles) for company assets and develop a clearer framework for background checks.
- **Background checks and vetting** as part of the recruitment process is the first step to prevent people with malicious intent to join the company. Clear criteria for applicants, background checks and potentially vetting help screening at the moment of employment, but it has to be noted that such screening only represents a snapshot of the past.
- A clear and protocolled **credential management** including an exit procedure helps managing keys, passwords, access codes, etc., also ensuring the cancellation of access to asset, systems, and information when staff members are changing positions or are leaving the company.
- **Insider threat awareness training** can help familiarising personnel with potential damage that can could be created by malicious intent, non-compliance or using personal vulnerabilities. During employment, **awareness campaigns** can help to remind staff of the potential damage to passengers, staff and business that could be caused by insiders.

INFORMATION AND CYBER SECURITY

Digitalisation is revolutionising the way we provide and consume services. Also in bus transport operations, it has brought innovative tools that make processes such as planning or maintenance more efficient. It also helps create new customer channels and services. Consequently, besides physical company assets, also digital assets and processes must be considered in security plans and concepts.

Information security focuses on protecting sensitive data and information from unauthorised access. This includes, but is not limited to, personal and financial information concerning staff or customers, corporate information, or information concerning business processes, such as staff rosters or maintenance schedules. Breaches of information security could lead to economic and reputational damage.

- Sensitive information should be kept under lock and key, ideally only be stored and processed within facilities with restricted access.
- Access rights should only be granted to relevant staff members. Credentials and passwords need to be regularly renewed.

Cyber security focuses on the integrity of IT and computer-supported systems. A cyber-attack has the potential to disrupt daily operational activities and might compromise safety systems, potentially putting the life of staff and passengers at risk. It is important to notice that also cyber security is a corporate challenge that should be part of an enterprise security culture. It should not be left to the IT department alone.

- Where possible, also digital assets should be physically protected from unauthorised access with locks, seals, covers and installing them within restricted access facilities.
- Physical access should be granted to relevant staff members only.
- Password levels and renewal requirements need to be defined in cooperation with the IT department.
- System integrity needs to be ensured with correct set-up, continuous managing and patching of software systems in line with provider recommendations. System maintenance and spare part management needs to ensure system integrity.
- Systems should be constantly monitored for anomalies. A special challenge in the cyber security context is that systems may be compromised and it is not discovered.

With new technologies being implemented in bus operations, such as e-buses or charging stations, new cyber security risks need to be considered. Systems delivered as assembled units may contain components sealed by the supplier. Assessing the risk potentially posed by malfunctioning or compromised system elements is a challenge to be addressed in future risk assessments.

THIRD PARTY SECURITY

Security risk management cannot be limited to the inside of an organisation. Business partners may share assets, suppliers and service providers may have temporary or permanent access to company facilities and systems, sub-contractors may oversee business processes (e.g., maintenance or administrative roles).

It is crucial to make third party security policies part of the selection process and to have clear agreements, rules, and monitoring policies in place.

(7)

SECURITY TRAINING

Security in bus operations is the responsibility of all staff members. Training programmes need to clarify the role and responsibility of staff at every position and provide employees with the expertise needed for their job.

Initial operational security training courses should provide the general skills and knowledge expected in every position. Recurrent operational security training programmes can be used to refresh specific know-how.

TRAINING NEEDS

Staff should receive operational security training to ensure they are aware of their security responsibility and how to respond to an attack appropriately.

- The responsibility of **operational and frontline staff** typically includes to be vigilant for and report suspicious situations, to handle conflicts and de-escalate, to respond to an incident when necessary.
- **Employees in locations with restricted access**, such as control rooms or depots, need to be aware of the access policy of the site they work in, and if applicable be able to register visitors and issue badges.
- The focus for **control room staff** is the handling of emergency calls or incoming threats and potential activation of security protocols.

TRAINING RECORDS

In order to keep an overview of security training provided and to plan needed refresher courses, it is recommended to maintain training records for all personnel, detailing:

- The date and content of the initial training attended;
- Training topics and session dates of refresher courses;
- Any special skill trained.

It is also recommended to have training records signed by the attendees, confirming to have received the training.

EXERCISES

Regular security exercises help monitor the level of preparedness within an organisation and understand shortcomings and vulnerabilities.

- **Internal table-top exercises** can be used to simulate the response to specific incidents and practice the activation of the crisis management organisation.
- **Table-top exercises with external partners** can help to align plans, procedures, and responsibility.
- **Live exercises** should also involve all relevant external partners. They are also crucial to ensure that first responders are familiar with infrastructure layout, rolling stock and safety regulations of bus operations.

Security in bus operation is the responsibility of all staff members.

(8)

EMERGENCY MANAGEMENT

CRISIS MANAGEMENT

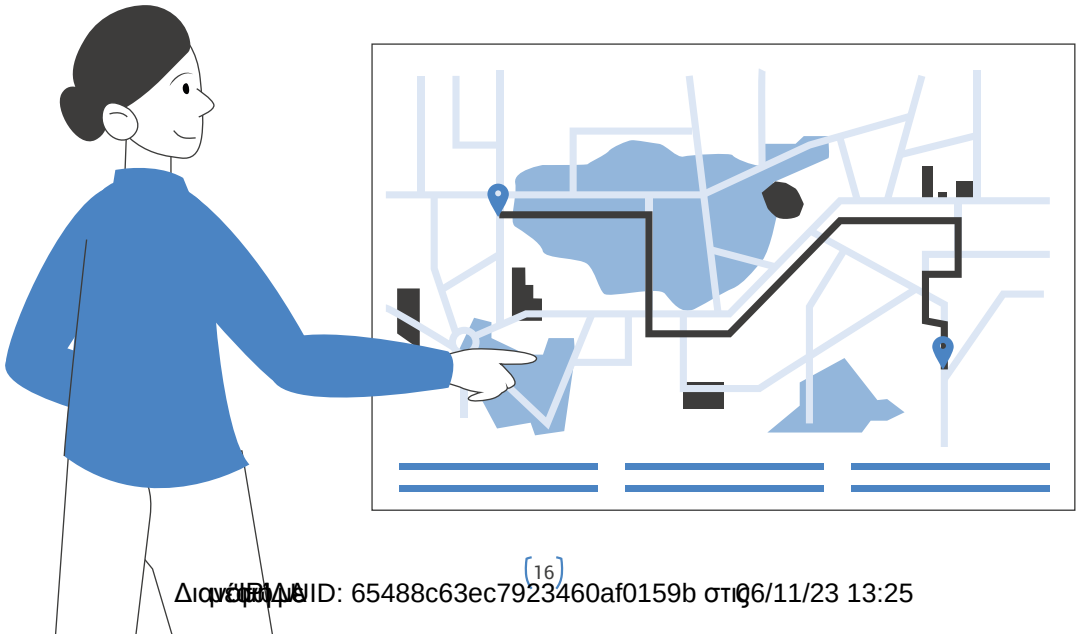
Given the complexity of transport systems and the flexibility of bus operations, crisis management comprises the handling of a crisis itself, but also managing the impact of a crisis at one location on the rest of the operation. Having to deal with a crisis does not mean an automatic shut-down of the entire operation as too many people depend on the availability. A crisis cell should be formally established. It should involve all departments of the organisation and be able to be activated with minimum delay to take charge of crisis management.

- A **crisis management plan** clarifies the roles and responsibilities of all departments within crisis management and operational management in degraded modes, involving re-routed bus lines and truncated services.
- A **crisis communication plan** needs to be prepared, which helps to deal with the media attention following any incident.

BUSINESS CONTINUITY

Besides handling the actual incident, emergency management also needs to consider business continuity aspects- adapting and re-routing services where possible and informing passengers about available services. Business continuity planning should include:

- **Back-up facilities** for critical functions (vehicle parking or maintenance, provisional bus stops, or customer service facilities) should be identified, which could be used to continue the operation in case that standard facilities are no longer operational or cannot be accessed.
- **Alternative routes** or a truncated bus network should be outlined to respond to disturbances and incidents along the route or partial unavailability of the bus fleet.
- Outlining **replacement bus services** can also help to support less flexible modes of transport, such as rail or metro, in case of events or major disruptions of the mobility network.



(9)

TRAINING GUIDELINES

INTRODUCTION

This chapter focuses on a basic security training lesson for operational public transport staff. The lesson aims to improve general security awareness, clarify the role and responsibility of operational staff, encourage to contribute, and provide the confidence to take the right action. It outlines the skills and competences that are needed to:

- Contribute to ensuring that public transport premises are controlled and managed spaces;
- Recognise suspicious situations and understand how to report them;
- React to emergencies, protecting passengers without compromising their own safety.

These training guidelines are developed around a number of basic scenarios, where operational staff are most likely to be the first people to be confronted and required to intervene. These are aligned with 'the SAFE BUS' Deliverable 4.1 "Driver's guide-book on security in public transport", which can be handed out to staff as a reference.

These training guidelines are developed around a number of basic scenarios.

TRAINING CONTENT

ANTI-TERRORISM

The introductory part of the training session should explain what terrorism is and why it is an important topic for public transport operators.

Terrorism means the use of violence or other criminal acts as justified means to achieve political goals. The objective is to frighten people, weaken communities, or destabilise economies.

Unfortunately, public transport systems have repeatedly been the target of terrorist activities, aiming to disrupt operations and sabotage mobility services.

Potential targets for terrorist activities could be our vehicles and infrastructure, such as stations, depots and workshops, customer centres or administrative buildings. The objective could also be to cause harm to people using public transport.

As transport providers, we are responsible for the safety and wellbeing of our passengers. This includes monitoring for suspicious situations and activities and reporting observations, as well as being able to handle emergencies and threats.

Reference 1 – Driver handbook "Anti-terrorism"

PREVENTION

This section should outline how some basic "housekeeping" can contribute to avoiding unauthorised access to restricted public transport facilities and assets and how to monitor for unusual situations.

It is important to remind participants that the required attention is nothing additional to their professional role and that they are not expected to act outside organisational policies and procedures.

A key protection measure is avoiding unauthorised access to restricted facilities. This includes depots, workshops, locker rooms and administrative buildings, but it also concerns the driver position of vehicles.

- If you see an **unfamiliar person** at a depot or site, check who they are and offer assistance.
- **Ensure your doors are closed** every time you leave a vehicle unattended.

Public facilities, such as stations, bus stops or customer centres have limited access control. Here, it is important to watch out for unusual behaviour or situations.

- **Be alert** for people acting suspiciously and nervously on buses, at stations or stops.
- **Check your vehicle regularly** for suspicious items and lost property every time you leave the depot as often as possible between journeys and every time you return to the depot.

Reference 2 - Driver handbook – "Prevention"

SUSPICIOUS SITUATIONS

The section aims to enable participants recognising suspicious situations and encourage them to report such situation. It is important to remind participants that they should not take risks and their safety is a priority. The basic scenarios selected for this training are addressed in two parts:

- How to recognise this situation as suspicious?
- What to do if there is reason for concern?

Response procedures suggested below are generic and aim to provide a general guideline. They can be amended to be aligned with existing company policies.

The following situations have been selected:

HOSTILE RECONNAISSANCE

A critical step in preparing any criminal activity is hostile reconnaissance. Hostile reconnaissance means gathering information about our facilities and operations that could be exploited in an attack. Critical information may be gathered by observing or directly approaching staff for information.

Indicators for hostile reconnaissance include:

- **Taking photographs** or videos of stations or other company facilities;
- **Repeated** or unusually extended presence of persons at stations without taking any bus service;
- **Attempting** to enter restricted facilities or bypass security measures, such as gates and fences;
- **Asking** inappropriate or unusual questions about security measures or operational procedures.

If you observe behaviour not in line with common daily passenger activities, follow these instructions:

Offer assistance	*If you feel safe, approach the person, and offer assistance.*
Inform dispatching	*Provide details of the incident or your concern to be recorded.*

Reference 3 - Driver Handbook "Hostile Reconnaissance"

SUSPICIOUS ITEMS

Passengers frequently leave luggage or items behind. However, abandoned items may be deliberately left behind and contain dangerous substances, such as explosives or chemicals.

Abandoned items should only be collected and handed over to the lost property service if there is no reason for concern. The No-touch protocol helps identifying suspicious items.

A suspicious item is an abandoned item that has any of the following characteristics:

NO-T	**Not typical of the surroundings (not likely to be lost property)**
OU	**ObvioUsly has suspicious characteristics (item is wet or dirty, has a strange smell, is closed with rope or tape)**
C	**Circumstances are suggesting concern (left behind in a busy environment, covered with powder, has visible cable or aluminium foil)**
H	**Deliberately hidden (no reason to be here, placed in an unusual location – under a seat or next to a trash bin)**

In case you locate an item that gives reason for concern, follow these instructions:

- ✓ ***DO** look for suspicious signs from a distance!*
- ✓ ***DO** alert the OCC and provide relevant details on the item! (Exact location, shape, size...)*
- ✓ ***DO** try to locate the owner!*
- ✓ ***DO** warn persons nearby & instruct them to move away!*
- ✓ ***DO** observe the item from a distance until the arrival of security staff!*
- ✗ ***DO NOT** touch, shake or open the item!*
- ✗ ***DO NOT** use a communications device or mobile phone near the suspicious item!*
- ✗ ***DO NOT** smoke near the item!*
- ✗ ***DO NOT** create panic among the public present at the site!*
- ✗ ***DO NOT** use metallic items in the vicinity!*

Reference 4 - Driver handbook "Suspicious items"

Stay vigilant but be aware of biases when assessing potential threats. Don't let preconceptions influence your judgment in potentially dangerous situations.

SUSPICIOUS PASSENGER BEHAVIOUR

Suspicious signs could come from the appearance or behaviour of passengers and include indicators, such as:

- Inappropriate clothing for the place, time and local conditions;
- Baggage that is incompatible with the overall appearance;
- Baggage that is disproportionally heavy.
- Nervousness or fear;
- Covert contact with other passengers;
- Refusing to cooperate with staff;
- Unjustified presence or loitering.

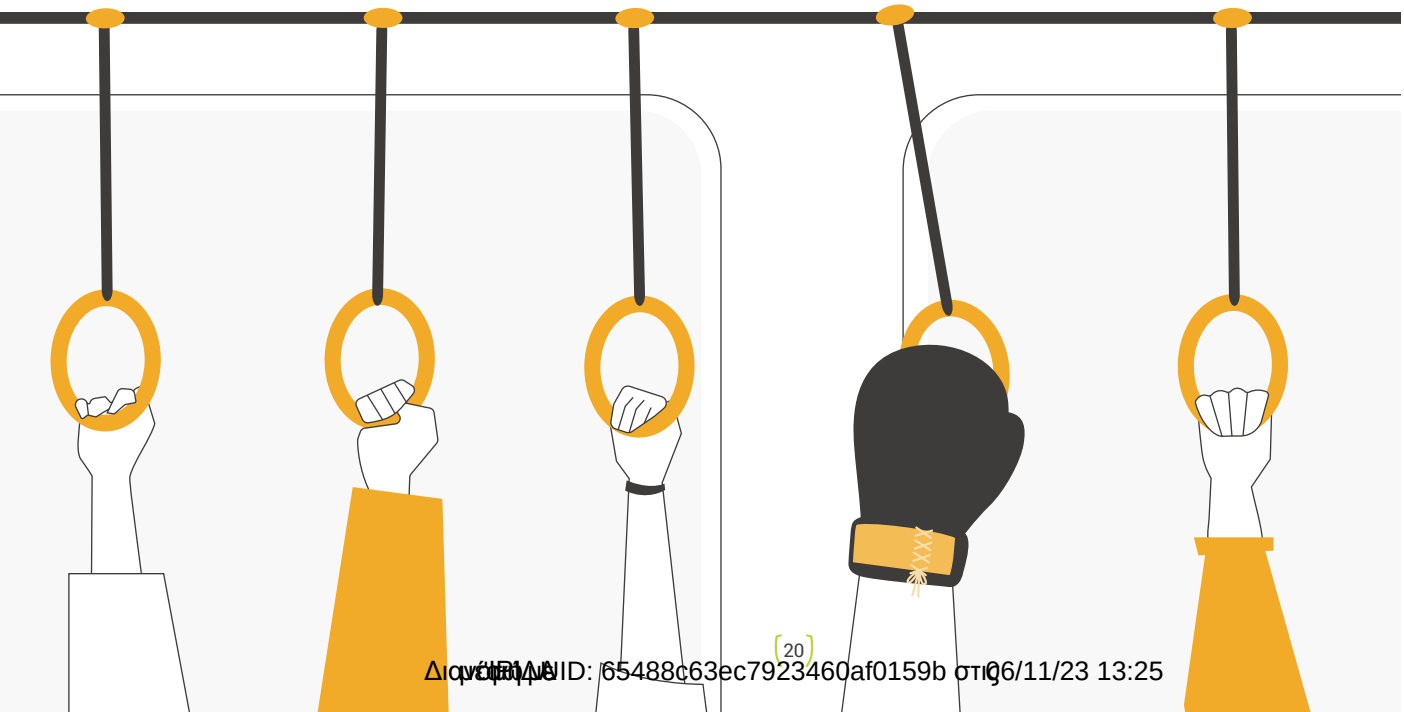
If passenger behaviour gives you reason for concern, follow these instructions:

Stop vehicle!	*Stop at a safe place, switch off the engine and stay calm. Inform passengers suggesting a vehicle fault.*
Contact dispatch!	*Report your concern and describe the situation.*
Evacuate vehicle!	*Evacuate yourself and your passengers to a safe distance!*
Monitor passenger	*Maintain observation of the suspicious passenger from a safe distance if possible!*
Wait for assistance	*Remain until a responsible person confirms that you may leave.*

Reference 5 - Driver handbook "Suspicious passenger behaviour"

Participants should be explained how reports will be verified and processed. It is important to explain why no visible follow-up may happen (verification with CCTV cameras, planned repair works, etc.). It is also important to include in the training how to recognise and be aware of one's biases when assessing potential threats.

Related training for staff members processing reports of suspicious situations from operational staff should always include a recognition of the attention paid and report submitted to encourage people to remain attentive and cooperate.



EMERGENCIES

The final section provides instructions on how to respond to emergencies, mainly for customer-facing employees. Again, it is important to remind participants that they should not take risks and their safety is a priority. It is recommended to base any instruction, after generating an alarm, on the Run-Hide-Report principle.

- **PUSH ALARM** – whenever possible, alert dispatch to be aware of the emergency and to initiate the appropriate response.
- **RUN** – get away from the danger as quickly as possible.
- **HIDE** – stay out of sight.
- **REPORT** – call dispatch with more details as soon as it is safe.

Response procedures suggested below are generic and aim to provide a general guideline. They can be amended to be aligned with existing company policies.

The following scenarios have been selected:

ATTACK ON BOARD

In the event of an immediate threat to yourself and/or the life and health of passenger, follow these instructions:

Push alarm!	*Push the alarm button.*
Open doors!	*Stop the vehicle to allow passengers to escape. Instruct them to leave if possible.*
Run and hide!	*Get away from danger and mute your phone.*
Report details!	*Once hidden, call dispatch with more information.*

Reference 6 - Driver Handbook "Attack on board"

ATTACK OUTSIDE THE VEHICLE

If you observe an attack at a stop or station, or your vehicle is being attacked from the outside, follow these instructions:

Push alarm!	*Push the alarm button.*
Do not stop!	*Keep driving and do not stop (if possible)! Inform the passengers.*
Call dispatch!	*Provide more details as soon as possible.*

Reference 7 - Driver Handbook "Attack outside the vehicle"

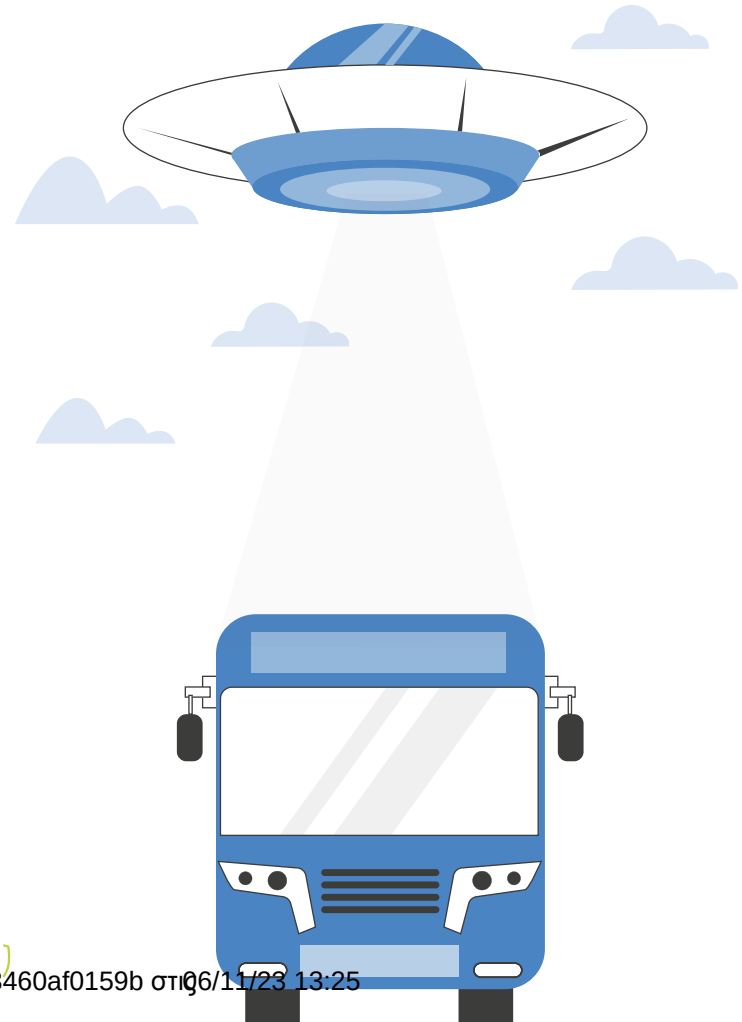
HIJACKING AND HOSTAGE-TAKING

In the event of a hijacking, a hostage-taking or a situation that threatens yourself and/or the life and health of your passengers, follow these instructions:

Push alarm!	*Push the alarm button.*
Keep calm!	*Don't resist, don't argue, obey instructions of the offender.*
Avoid attention!	*Avoid drawing attention to yourself, avoid eye contact, make no sudden movements.*

Reference 8 - Driver Handbook "Hijacking and hostage-taking"

Always remember, your safety is a priority.



NOTES